Network Device Interpretation # 201832

FCS_SSHC_EXT.1.5, Test 1 - Server and client side seem to be confused

Status: ☒ *Active* ☐ *Inactive*

Date: *18-Mar-2019*

End of proposed Transition Period (to be updated after TR2TD process): *18-Apr-2019*

Type of Change: ☐ Immediate application ☒ Minor change ☐ Major change

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *NDcPP V2.0e, NDcPP V2.1, FWcPP V2.0e, ND SD V2.0e, ND SD V2.1*

Affected Section(s): *FCS_SSHC_EXT.1.5, Test 1*

Superseded Interpretation(s): *None*

Issue:

The FCS_SSHC_EXT.1.5 SFR in collaborative protection profile for network devices v2.0 + Errata 20180314 states:

The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: ssh-rsa, ecdsa-sha2-nistp256] and [selection: ecdsa-sha2- nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, no other public key algorithms] as its public key algorithm(s) and rejects all other public key algorithms

While the Test 1 in the supporting document for the same requirement is:

Test 1: The evaluator shall establish a SSH connection using each of the public key algorithms specified by the requirement to authenticate an SSH server to the TOE. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

The SFR states that the selected algorithms should be used by the TOE 'as its public key algorithms'—in this case on the client side. However, the AA is written such that the algorithms should be used on the server side via 'using each of the public key algorithms specified by the requirement to authenticate an SSH server to the TOE'

It appears that the AA needs to be rewritten to accommodate the expected client side functionality of the TOE.

Since different public key algorithms can be used for server side and client side of the same connection, consideration should be taken to rewriting the requirement to represent what algorithms the client will allow a server to use to authenticate to the TOE.

Resolution:

The NIT acknowledges the issue described in the Issue section but does not regard a rewrite of the test requirement as necessary. The following test objective definition shall be added to the definition of Test 1 for FCS_SSHC_EXT.1.5 to enhance clarity:

<new> *Test objective: The purpose of this positive test is to check the authentication of the server by the client (when establishing the transport layer connection), and not for checking generation of the authentication message from the client (in the User Authentication Protocol). The evaluator is therefore intended to establish sufficient separate SSH connections (with an appropriately configured server) to cause the TOE to demonstrate use of all public key algorithms claimed in FCS_SSHC_EXT.1.5 in the ST.* </new>

Rationale:

The added sentence clarifies the intention of the test.

Further Action:

None.

Action by Network iTC:

None.